REMARKS

Claims 1, 2 and 4-6 are pending in the above-identified patent application. Claims 1 and 5 have been amended by way of the present amendment. Reconsideration is respectfully requested.

In the outstanding Office Action, claims 1 and were rejected to under 35 U.S.C. § 112, second paragraph; and claims 1, 2 and 4-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,604,807 (Yamaguchi et al.) in view of "Transparent Network Security Policy Enforcement" (Keromytis et al) and U.S. Patent No. 7,117,361 (Hild). Reconsideration is respectfully requested.

35 U.S.C. § 112 Claim Rejections

Claims 1 and 5 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

Claim 1 has been amended to clarify the invention. In particular, claim 1 has been amended to provide proper antecedent basis for the phrase "plurality of ports." However, it is respectfully submitted that claim 5 does provide proper antecedent basis for this phrase. Therefore, it is respectfully submitted that the amendments raise no question of new matter and that claims 1 and 5, and claims dependent thereon are now definite.

35 U.S.C. § 103 Claim Rejections

Claims 1, 2 and 4-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamaguchi et al. in view of Keromytis et al. and Hild. Reconsideration is respectfully requested.

Claims 1 and 5 have been amended to clarify the invention. In particular, claim 1 has been amended to recite:

> ~~a plurality of communications terminals for performing data communications;~~
>
> an encryption apparatus which can be connected between ~~the~~ a plurality of communications terminals, the plurality of communications terminals for performing data communications;
>
> the apparatus including encryption/decryption means for performing an encrypting process and a decrypting process on data to terminate encryption-based security between the communications terminals having the encrypting capability and the non-encrypting capability; and
>
> a manager terminal for inputting information for the presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key into each of the encryption apparatus and the communications terminals remotely from the manager terminal over a network, so that settings for the encrypted data communications on each of the apparatus and the terminals are completed,
>
> wherein the various information includes at least one of ~~the presence/absence of the encrypting/decrypting process, the communicability indicating that a packet is~~ instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received, ~~the encryption level,~~ and the time period for the encryption~~, the encryption policy for each division~~;
>
> wherein the plurality of communications terminals, the manager terminal, and the encryption apparatus are connected via a cable or wireless network;
>
> wherein the encryption apparatus further includes bridge means for allowing data to be outputted as it is from another port without any routing process; and
>
> wherein the data ~~has been~~is received with one of ~~the~~ a plurality of ports of the encryption apparatus and the encrypting or decrypting process ~~has been~~is performed on the data.

Claim 5 has been similarly amended. Support for the amendment is provided in the original application and figures. In particular, the specification of US Patent Application Publication US 2005/0008160 discloses:

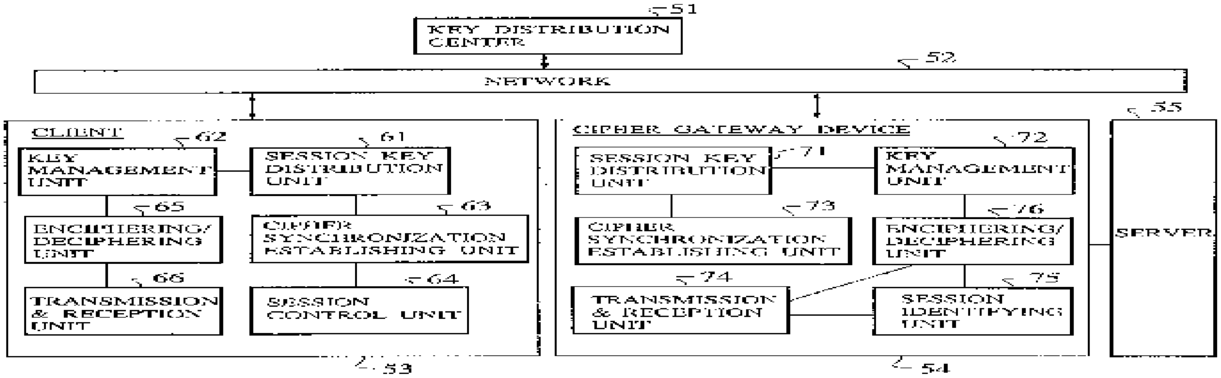
> a manager terminal **12** to each of the encryption apparatus **1** and the PCs **7-9** via the hub **5**, wherein examples of the information to be set by the manager terminal includes: (A)

> Information that instructs to perform the encrypting/decrypting process, or instructs not to perform the encrypting/decrypting process; (B) *Information for instructing to discard data packets (In particular, this information instructs to discard data packets, when data packets to be communicated between predetermined terminals have been received.)*; (C) Information for instructing a security level of the encryption; (D) Information for instructing time when data encryption is to be performed; (E) The encryption policy for each division; and (F) Information for encryption keys (emphasis added).[1]

Thus, in consideration of the above, it is respectfully submitted that the amendments do not raise any questions of new matter

Yamaguchi et al. discloses a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware, and establishing a synchronization at the start and end of the cipher communication.[2] In particular, Yamaguchi et al. discloses, as shown in **FIG. 12** below, wherein each client **53** and each cipher gateway device **54** are connected with the key distribution center **51**, the network **52**, and the server **55**.[3] Further, Yamaguchi et al. discloses the cipher gateway

FIG. 12


51
KEY DISTRIBUTION CENTER
52
NETWORK
CLIENT
62
61
KEY MANAGEMENT UNIT
SESSION KEY DISTRIBUTION UNIT
65
63
ENCIPHERING/DECIPHERING UNIT
CIPHER SYNCHRONIZATION ESTABLISHING UNIT
66
64
TRANSMISSION & RECEPTION UNIT
SESSION CONTROL UNIT
53
CIPHER GATEWAY DEVICE
71
72
SESSION KEY DISTRIBUTION UNIT
KEY MANAGEMENT UNIT
73
76
CIPHER SYNCHRONIZATION ESTABLISHING UNIT
ENCIPHERING/DECIPHERING UNIT
74
75
TRANSMISSION & RECEPTION UNIT
SESSION IDENTIFYING UNIT
54
55
SERVER

[1] U.S. Patent Application Publication No. 20050008160 at paragraphs **[0035]** to **[0041].**

[2] Yamaguchi et al. at ABSTRACT.

[3] *Id.* at **FIG. 12**; and column 10, lines 53-56.

device **54** or router receives the packet destined to the server **55** from the client **53**, and deciphers the packet by using the common session key Ks and that this deciphered packet (plain text packet) is transmitted to the server **55** to carry out the non-cipher communication between the cipher gateway device **54** and the server **55**.[4] Alternatively, Yamaguchi et al. discloses the cipher gateway device **54** or router receives the packet destined to the client **53** from the server **55** by the non-cipher communication, and enciphers the packet by using the common session key Ks and this enciphered packet is transmitted to the client **53** to carry out the cipher communication between the cipher gateway device **54** or router and the client **53**.[5]

However, Yamaguchi et al. nowhere discloses, as amended claims 1 and 5 recite: disclose, as amended claims 1 and 5 recite:

> wherein the various information includes at least one of *instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received, and the time period for the encryption* (emphasis added).

That is, "instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received" or "the time period for the encryption" is *not* disclosed by either in Yamaguchi et al. and Keromytis et al. Thus, it is respectfully submitted that Yamaguchi et al. does not disclose these limitations of the claimed invention.

In addition, the outstanding Office Action acknowledges other deficiencies in Yamaguchi et al. and in the combination of Yamaguchi et al. and Keromytis et al. and attempts to overcome these deficiencies by combining and Hild with Yamaguchi et al. and Keromytis et al.[6] However, neither Keromytis et al. nor Hild can overcome all of the deficiencies of Yamaguchi et al. or the combination of Yamaguchi et al. and Keromytis et al.[7], as will be discussed below.

[4] *Id.* at **FIG. 12**; and column 12, lines 50-56.

[5] *Id.* at **FIG. 12**; and column 12, lines 57-63.

[6] See outstanding Office Action at page 4, lines 15-20; and page 5, lines 8-11.

[7] See outstanding Office Action at page 4, lines 15-20; and page 5, lines 8-11.

Keromytis et al. discloses recent work in the area of the network security, such as IPsec, provides mechanisms for securing the traffic between any two interconnected hosts.[8] However, Keromytis et al. does not disclose the mechanism of the central encryption management, but just the combinations between encryption communications and bridges. However, neither Yamaguchi et al. or Keromytis et al. disclose, as amended claims 1 and 5 recite:

> wherein the various information includes at least one of *instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received, and the time period for the encryption* (emphasis added).

That is, "instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received" or "the time period for the encryption" is *not* disclosed by either in Yamaguchi et al. and Keromytis et al. Thus, Keromytis et al. cannot overcome all of the deficiencies of Yamaguchi et al. Therefore, neither Yamaguchi et al. or Keromytis et al., whether taken alone or in combination, disclose all of the limitations of the claimed invention.

In addition, Hild discloses a method of transmitting information data from a sender to a receiver via a transcoder.[9] In particular, as shown in **FIG. 1** below, Hild discloses a sender **1**, also called client, is connected via a communication connection, which need not be a physical connection, to a receiver **3** via a transcoder **2**, wherein policy information **17** is accessible for the sender **1**, the transcoder **2** and the receiver **3**. In addition, Hild discloses the sender **1** comprises a divisor means **21** for subdividing information data **9**, denoted with **ID**, which is to be sent to the receiver **3** and that the output of the divisor means **21** is confidential information data **16**, denoted with **CD**, and non-confidential information data **15**, denoted as **NCD**. Further, Hild discloses an encryptor **5** that is arranged for encrypting the confidential information data **16** and delivers encrypted confidential information data **14**, denoted as **ECD**. Furthermore, Hild discloses the transcoder **2** comprises decision means **4**, denoted with **TC**, for deciding which part of the received partly encrypted information data **14, 15** is to be transcoded before transmitting it to the receiver **3**.

[8] Keromytis et al. at ABSTRACT.
[9] Hild at ABSTRACT.

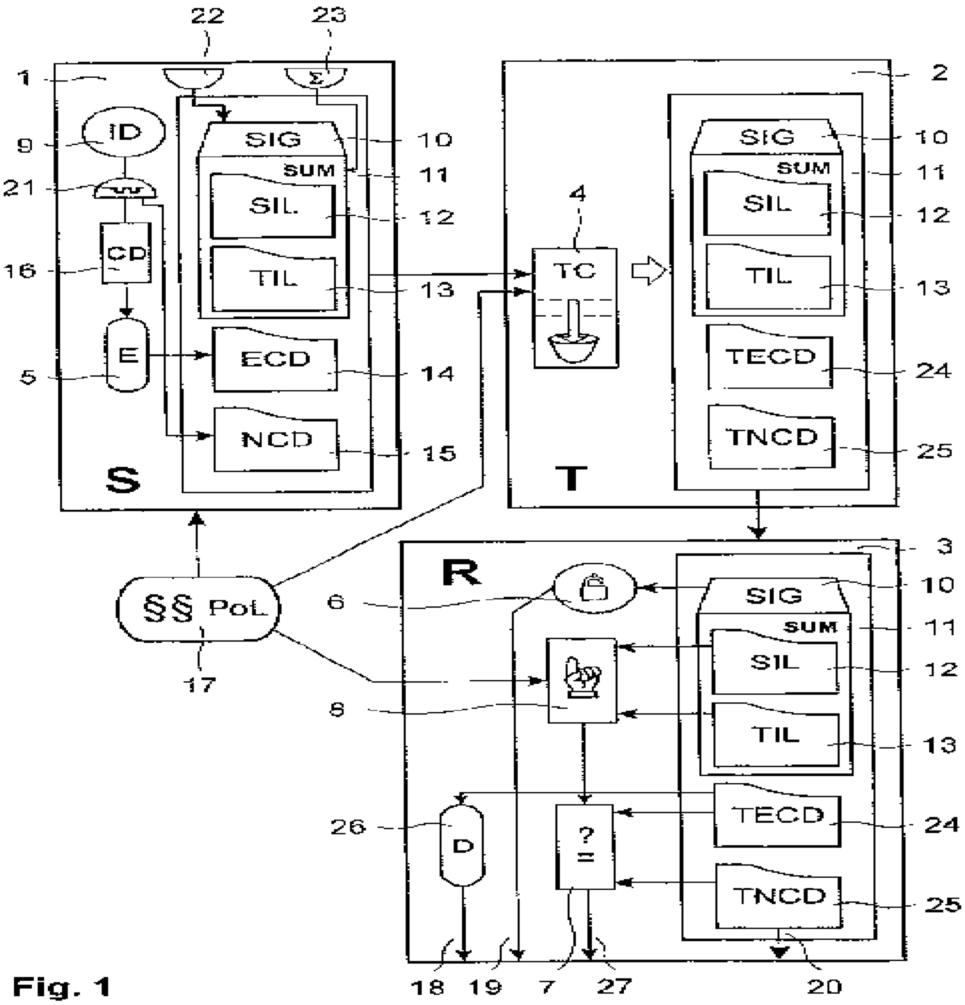


Fig. 1

However, neither Hild nowhere discloses, as amended claims 1 and 5 recite:

> wherein the various information includes at least one of *instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received, and the time period for the encryption* (emphasis added).

That is, "instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received" or "the time period for the encryption" is *not* disclosed by either in Hild. Thus, Hild cannot overcome all of the deficiencies of Yamaguchi et al. and Keromytis et al., Therefore, it is respectfully submitted that none of Yamaguchi et al., Keromytis et al. or Hild, whether taken alone or in combination, disclose all of the limitations of the claimed invention, and that amended claims 1 and 5, and claims dependent thereon, patentably distinguish thereover.

Conclusion

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01101-US1 from which the undersigned is authorized to draw.

Dated: October 31, 2008 Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Agent for Applicant